PCT / IB 9 9 / 0 1 3 2 3
16. 08. 99

Europäisches Patentamt | European Patent Office | Office européen des brevets

5

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

98401870.5

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

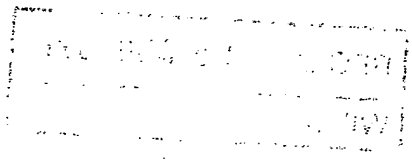
For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

Arlette Fiedler

A. Fiedler

DEN HAAG, DEN
THE HAGUE,
LA HAYE, LE 14/07/99



THIS PAGE BLANK (USPTO)

Eur päisches Patentamt
European Patent Office
Office eur péen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.:
Demande n°: 98401870.5

Anmeldetag:
Date of filing:
Date de dépôt: 22/07/98

Anmelder:
Applicant(s):
Demandeur(s):
CANAL+ Société Anonyme
75711 Paris Cedex 15
FRANCE

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
Method and apparatus for secure communication of information between a plurality of digital audiovisual devices

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat: State: Pays:	Tag: Date: Date:	Aktenzeichen: File no. Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
H04N7/167, H04L29/06

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE
Etats contractants désignés lors du depôt:

Bemerkungen:
Remarks:
Remarques:

METHOD AND APPARATUS FOR SECURE COMMUNICATION OF INFORMATION BETWEEN A PLURALITY OF DIGITAL AUDIOVISUAL DEVICES

The present invention relates to a method and apparatus for secure communication of information between a plurality of digital audiovisual devices connected in a network.

The present invention is particularly applicable to the field of digital television, where scrambled audiovisual information is broadcast to a number of subscribers, each subscriber possessing a decoder or integrated receiver/decoder (IRD) capable of descrambling the transmitted program for subsequent viewing.

In a typical system, scrambled digital audiovisual data is transmitted together with a control word for descrambling of the digital data, the control word itself being encrypted by an exploitation key and transmitted in encrypted form. A decoder receives the scrambled digital data and encrypted control word which uses an equivalent of the exploitation key to decrypt the encrypted control word and thereafter descramble the transmitted data. A paid-up subscriber will receive periodically the exploitation key necessary to decrypt the encrypted control word so as to permit viewing of a particular program. Encryption and decryption keys are conventionally stored in a portable security module, such as a smart card used to personalise the decoder.

A particular problem arises in the case of a user who has two or more decoders since existing subscription management systems often have difficulty in opening a second subscription for the same person at the same address. Consequently, in such circumstances, it would be advantageous to allow two or more decoders to function using the same subscription.

The PCT patent application WO 97/35430 in the name of News Datacom Limited shows one possible solution to this problem. In this system, a pair of decoders are organised in a master/slave configuration. Subscription rights are managed by the master decoder and its associated smart card. In order to transfer rights to the slave decoder, the slave smart card must be inserted at regular

intervals in the master decoder. The disadvantage of this system is that a user is obliged to manually withdraw, recharge and replace the card in the slave decoder.

Other proposed solutions have included the generation of a duplicate smart card containing exactly the same rights as present in a master smart card. Such a solution is also undesirable, since it may not be wished to give exactly the same rights to multiple decoders and since the creation of a clone or duplicate card always incurs the risk fraud.

It is an object of the present invention in its general and specific embodiments to overcome some or all of the problems of these prior art systems.

According to the present invention there is providing a method of providing secure communication of information between at least a first and second digital audiovisual device and characterised in that the second device receives a certificate comprising a transport public key encrypted by a management private key, the second device decrypting the certificate using an equivalent management public key and thereafter using the transport public key to encrypt information sent to the first device, the first device using an equivalent private key to decrypt the information.

In such a method, the first device assumes the role of a master device, personalised with a certificate generated using a management private key. The management private key is held in secret by the system manager and may not be derived from the information stored in the certificate. The second device assumes the role of a slave device. Information encrypted by the transport public key held by the second device may only be decrypted by the equivalent private key held by the first device. As will be described below, this information may thereafter be used to set up a secure bi-directional link to transfer subscription rights and other information.

Advantageously, the transport private/public key pair are uniquely associated with the first and second device pair. This ensures complete security of encrypted messages transmitted to the first device.

As will be appreciated, whilst the use of unique keys enables an increased level of security it may be decided in some cases to use non-unique keys, for example, for different pairs of devic s distributed in different territories, where the security risk associated with such duplication is relatively low.

Preferably, the encrypted information sent by the second device comprises a session key, in particular, a session key generated by the second device and usable in conjunction with a symmetric encryption algorithm. This key, which may be generated at the initiation of a communication session for transfer of subscription can thereafter be used for bi-directional communication of information between the first and second devices.

In an alternative embodiment a session key pair corresponding to a private/public key pair of an asymmetric algorithm may be used.

The advantage of a changeable symmetric session key lies in the increased level of security that such a key provides as well as the possibility of bi-directional communication that it enables. Other embodiments are nevertheless possible, for example, in which transmission related information is directly encrypted using the transport public key held by the second device.

In one embodiment, the session key is used by the first device to encrypt control word information subsequently communicated to the second device. In such an embodiment, the second device decrypts the control word information using the equivalent session key and thereafter descrambles an associated transmission or programme for display.

In one embodiment, prior to the communication of the first certificate, the second device receives a secondary system certificate comprising the management public key encrypted by a system private key, the second device decrypting the system certificate using a system public key so as to obtain the management public key used thereafter to decrypt the encrypted transport public key.

This embodiment may be implemented, for example, where a different source for the first and second devices exists. The system private key may be held in secret by, for example, the source of the

second device. A system certificate will only be issued in the event that the second device source is sure of the integrity of security at the first device source. Thereafter, a designated first device source will embed this certificate in all first device smart cards, such that a second device smart card can authenticate the origin of such cards.

As will be understood, the second device source need only know the management public key of the first device source in order to generate a system certificate and neither party needs to share its private encryption keys in carrying out these certifying operations.

The secure communication link between the devices may be used to convey many different types of information, including different information relating to descrambling a transmission or even other matters. In particular, whilst the above embodiments discuss the use of a session key in the encryption and communication of control word information, other embodiments are possible. For example, audio and/or visual data to be recorded may be directly encrypted by the first device using a session key and communicated directly to the second device for decryption and display.

Other embodiments may use the secure communication link to transfer, for example, exploitation keys present in the first device such that the second device can carry out all operations to decrypt control word information and descramble a transmission in the same manner as the first device.

Whilst the above description has described encryption and decryption operations in relation to a first and second device it is to be understood that these operations and, in particular the keys needed in such operations, need not necessarily managed or held by elements permanently integrated in the devices themselves.

In particular, in a preferred embodiment, the first and second devices further comprise first and second portable security modules used to carry out some or all of th encryption or decryption steps described above.

Such portable security devices can take any convenient form depending on the physical size and characteristics of the device. For example, whilst in some cases a smart card equivalent to a bank card may be used, other formats such as PCMCIA type cards are equally possible.

The physical communication link between the two devices may take many forms, for example, a radio, telephone or infra-red link. However, preferably, the communication link is implemented by connection of the first and second decoders on a bus, for example, a IEEE 1394 bus link.

Whilst the invention has been described with reference to a first and second device, it will be appreciated that the same principal may be used to set up a chain of communication between a series of such devices, e.g. between a single master device and a plurality of slave devices.

The present invention is particularly, but not exclusively, applicable to the implementation of secure communication link between a first and second decoder. However, other applications of the invention for use with other digital audiovisual devices may be envisaged, for example, to encrypt information from a decoder to a digital VCR, between two digital VCRs etc.

The present invention is particularly but not exclusively adapted for use with a digital television transmission system in which the decoders are adapted to receive a digital television transmission.

The present invention has been described above in relation to a method of communication. The invention equally extends to a first and second device adapted for use in such a method and one or more portable security modules adapted for use in such a system.

Suitable algorithms for use in this invention for generating private/public keys may include, for example, RSA or Diffie-Hellman, and suitable symmetric key algorithms may include DES type algorithms, for example. However, unless obligatory in view of the context or unless otherwise specified, no general distinction is made between keys associated with symmetric algorithms and those associated with public/private algorithms.

The terms "scrambled" and "encrypted" and "control word" and "key" have been used at various parts in the text for the purpose of clarity of language. However, it will be understood that no fundamental distinction is to be made between "scrambled data" and "encrypted data" or between a "control word" and a "key". Similarly, the term "equivalent key" is used to refer to a key adapted to decrypt data encrypted by a first mentioned key, or vice versa.

The term "receiver/decoder" or "decoder" as used herein may connote a receiver for receiving either encoded or non-encoded signals, for example, television and/or radio signals, which may be broadcast or transmitted by some other means. The term may also connote a decoder for decoding received signals. Embodiments of such decoders may also include a decoder integral with th receiver for decoding the received signals, for example, in a "set-top box", a decoder functioning in combination with a physically separate receiver, or such a decoder including additional functions, such as a web browser or a video recorder or a television.

As used herein, the term "digital transmission system" includes any transmission system for transmitting or broadcasting for example primarily audiovisual or multimedia digital data. Whilst the present invention is particularly applicable to a broadcast digital television system, the invention may also be applicable to a fixed telecommunications network for multimedia internet applications, to a closed circuit television, and so on.

As used herein, the term "digital television system" includes for example any satellite, terrestrial, cable and other system.

There will now be described, by way of example only, a number of embodiments of the invention, with reference to the following figures, in which:

Figure 1 shows the overall architecture of a digital TV system according to this embodiment;

Figure 2 shows the architecture of the conditional access system of Figure 1;

Figure 3 shows the encryption levels in the conditional access system;

Figure 4 shows the layout of a first and second decoder;

Figure 5 shows the steps associated with setting up a secure communication link between the first and second decoder; and

Figure 6 shows the operation of the first and second decoder in transferring control word information via the secure communication link.

An overview of a digital television broadcast and reception system 1 is shown in Figure 1. The invention includes a mostly conventional digital television system 2 which uses the MPEG-2 compression system to transmit compressed digital signals. In more detail, MPEG-2 compressor 3 in a broadcast centre receives a digital signal stream (for example a stream of audio or video signals). The compressor 3 is connected to a multiplexer and scrambler 4 by linkage 5. The multiplexer 4 receives a plurality of further input signals, assembles one or more transport streams and transmits compressed digital signals to a transmitter 6 of the broadcast centre via linkage 7, which can of course take a wide variety of forms including telecom links.

The transmitter 6 transmits electromagnetic signals via uplink 8 towards a satellite transponder 9, where they are electronically processed and broadcast via a notional downlink 10 to earth receiver 11, conventionally in the form of a dish owned or rented by the end user. The signals received by receiver 11 are transmitted to an integrated receiver/decoder 12 owned or rented by the end user and connected to the end user's television set 13. The receiver/decoder 12 decodes the compressed MPEG-2 signal into a television signal for the television set 13.

A conditional access system 20 is connected to the multiplexer 4 and the receiver/decoder 12, and is located partly in th broadcast centre and partly in the decoder. It enables the end user to access digital television broadcasts from one or more broadcast suppliers. A smartcard, capable of decrypting messages relating to commercial offers (that is, one or several television programmes sold by the

broadcast supplier), can be inserted into the receiver/decoder 12. Using the decoder 12 and smartcard, the end user may purchase events in either a subscription mode or a pay-per-view mode.

An interactive system 17, also connected to the multiplexer 4 and the receiver/decoder 12 and again located partly in the broadcast centre and partly in the decoder, may be provided to enable the end user to interact with various applications via a modemmed back channel 16.

The conditional access system 20 will now be described in more detail. With reference to Figure 2, in overview the conditional access system 20 includes a Subscriber Authorization System (SAS) 21. The SAS 21 is connected to one or more Subscriber Management Systems (SMS) 22, one SMS for each broadcast supplier, for example by a respective TCP-IP linkage 23 (although other types of linkage could alternatively be used). Alternatively, one SMS could be shared between two broadcast suppliers, or one supplier could use two SMSs, and so on.

First encrypting units in the form of ciphering units 24 utilising "mother" smartcards 25 are connected to the SAS by linkage 26. Second encrypting units again in the form of ciphering units 27 utilising mother smartcards 28 are connected to the multiplexer 4 by linkage 29. The receiver/decoder 12 receives a portable security module, for example in the form of "daughter" smartcard 30. It is connected directly to the SAS 21 by Communications Servers 31 via the modemmed back channel 16. The SAS sends, amongst other things, subscription rights to the daughter smartcard on request.

The smartcards contain the secrets of one or more commercial operators. The "mother" smartcard encrypts different kinds of messages and the "daughter" smartcards decrypt the messages, if they have the rights to do so.

The first and second ciphering units 24 and 27 comprise a rack, an electronic VME card with software stored on an EEPROM, up to 20 electronic cards and one smartcard 25 and 28 respectively, for each electronic card, one card 28 for encrypting the ECMs and one card 25 for encrypting the EMMs.

The operation of the conditional access system 20 of the digital television system will now be described in more detail with reference to the various components of the television system 2 and the conditional access system 20.

Multiplexer and Scrambler

With reference to Figures 1 and 2, in the broadcast centre, the digital audio or video signal is first compressed (or bit rate reduced), using the MPEG-2 compressor 3. This compressed signal is then transmitted to the multiplexer and scrambler 4 via the linkage 5 in order to be multiplexed with other data, such as other compressed data.

The scrambler generates a control word used in the scrambling process and included in the MPEG-2 stream in the multiplexer. The control word is generated internally and enables the end user's integrated receiver/decoder 12 to descramble the programme.

Access criteria, indicating how the programme is commercialised, are also added to the MPEG-2 stream. The programme may be commercialised in either one of a number of "subscription" modes and/or one of a number of "Pay Per View" (PPV) modes or events. In the subscription mode, the end user subscribes to one or more commercial offers, or "bouquets", thus getting the rights to watch every channel inside those bouquets. In the preferred embodiment, up to 960 commercial offers may be selected from a bouquet of channels.

In the Pay Per View mode, the end user is provided with the capability to purchase events as he wishes. This can be achieved by either pre-booking the event in advance ("pre-book mode"), or by purchasing the event as soon as it is broadcast ("impulse mode"). In the preferred embodiment, all users are subscribers, whether or not they watch in subscription or PPV mode, but of course PPV viewers need not necessarily be subscribers.

Entitlement Control Messages

Both the control word and the access criteria are used to build an Entitlement Control Message (ECM). This is a message sent in relation with a scrambled program; the message contains a control word (which allows for the descrambling of the program) and the access criteria of the broadcast program. The access criteria and control word are transmitted to the second encrypting unit 27 via the linkage 29. In this unit, an ECM is generated, encrypted and transmitted on to the multiplexer and scrambler 4. During a broadcast transmission, the control word typically changes every few seconds, and so ECMs are also periodically transmitted to enable the changing control word to be descrambled. For redundancy purposes, each ECM typically includes two control words; the present control word and the next control word.

Each service broadcast by a broadcast supplier in a data stream comprises a number of distinct components; for example a television programme includes a video component, an audio component, a sub-title component and so on. Each of these components of a service is individually scrambled and encrypted for subsequent broadcast to the transponder 9. In respect of each scrambled component of the service, a separate ECM is required. Alternatively, a single ECM may be required for all of the scrambled components of a service. Multiple ECMs are also generated in the case where multiple conditional access systems control access to the same transmitted program.

Entitlement Management Messages (EMMs)

The EMM is a message dedicated to an individual end user (subscriber), or a group of end users. Each group may contain a given number of end users. This organisation as a group aims at optimising the bandwidth; that is, access to one group can permit the reaching of a great number of end users.

Various specific types of EMM can be used. Individual EMMs are dedicated to individual subscribers, and are typically used in the provision of Pay Per View services; these contain the group identifier and the position of the subscriber in that group.

Group subscription EMMs are dedicated to groups of, say, 256 individual users, and are typically used in the administration of some subscription services. This EMM has a group identifier and a subscribers' group bitmap.

Audience EMMs are dedicated to entire audiences, and might for example be used by a particular operator to provide certain free services. An "audience" is the totality of subscribers having smartcards which bear the same conditional access system identifier (CA ID). Finally, a "unique" EMM is addressed to the unique identifier of the smartcard.

EMMs may be generated by the various operators to control access to rights associated with the programs transmitted by the operators as outlined above. EMMs may also be generated by the conditional access system manager to configure aspects of the conditional access system in general.

Programme Transmission

The multiplexer 4 receives electrical signals comprising encrypted EMMs from the SAS 21, encrypted ECMs from the second encrypting unit 27 and compressed programmes from the compressor 3. The multiplexer 4 scrambles the programmes and sends the scrambled programmes, the encrypted EMMs and the encrypted ECMs to a transmitter 6 of the broadcast centre via the linkage 7. The transmitter 6 transmits electromagnetic signals towards the satellite transponder 9 via uplink 8.

Programme Reception

The satellite transponder 9 receives and processes the electromagnetic signals transmitted by the transmitter 6 and transmits the signals on to the earth receiver 11, conventionally in the form of a dish owned or rented by the end user, via downlink 10. The signals received by receiver 11 are transmitted to the integrated receiver/decoder 12 owned or rented by the end user and connected to the end user's television set 13. The receiver/decoder 12 demultiplexes the signals to obtain scrambled programmes with encrypted EMMs and encrypted ECMs.

If the programme is not scrambled, that is, no ECM has been transmitted with the MPEG-2 stream, the receiver/decoder 12 decompresses the data and transforms the signal into a video signal for transmission to television set 13.

If the programme is scrambled, the receiver/decoder 12 extracts the corresponding ECM from the MPEG-2 stream and passes the ECM to the "daughter" smartcard 30 of the end user. This slots into a housing in the receiver/decoder 12. The daughter smartcard 30 controls whether the end user has the right to decrypt the ECM and to access the programme. If not, a negative status is passed to the receiver/decoder 12 to indicate that the programme cannot be descrambled. If the end user does have the rights, the ECM is decrypted and the control word extracted. The decoder 12 can then descramble the programme using this control word. The MPEG-2 stream is decompressed and translated into a video signal for onward transmission to television set 13.

Subscriber Management System (SMS)

A Subscriber Management System (SMS) 22 includes a database 32 which manages, amongst others, all of the end user files, commercial offers, subscriptions, PPV details, and data regarding end user consumption and authorization. The SMS may be physically remote from the SAS.

Each SMS 22 transmits messages to the SAS 21 via respective linkage 23 which imply modifications to or creations of Entitlement Management Messages (EMMs) to be transmitted to end users.

The SMS 22 also transmits messages to the SAS 21 which imply no modifications or creations of EMMs but imply only a change in an end user's state (relating to the authorization granted to the end user when ordering products or to the amount that the end user will be charged).

The SAS 21 sends messages (typically requesting information such as call-back information or billing information) to the SMS 22, so that it will be apparent that communication between the two is two-way.

Subscriber Auth rization System (SAS)

The messages generated by the SMS 22 are passed via linkage 23 to the Subscriber Authorization System (SAS) 21, which in turn generates messages acknowledging receipt of the messages generated by the SMS 21 and passes these acknowledgements to the SMS 22.

In overview the SAS comprises a Subscription Chain area to give rights for subscription mode and to renew the rights automatically each month, a Pay Per View Chain area to give rights for PPV events, and an EMM Injector for passing EMMs created by the Subscription and PPV chain areas to the multiplexer and scrambler 4, and hence to feed the MPEG stream with EMMs. If other rights are to be granted, such as Pay Per File (PPF) rights in the case of downloading computer software to a user's Personal Computer, other similar areas are also provided.

One function of the SAS 21 is to manage the access rights to television programmes, available as commercial offers in subscription mode or sold as PPV events according to different modes of commercialisation (pre-book mode, impulse mode). The SAS 21, according to those rights and to information received from the SMS 22, generates EMMs for the subscriber.

The EMMs are passed to the Ciphering Unit (CU) 24 for ciphering with respect to the management and exploitation keys. The CU completes the signature on the EMM and passes the EMM back to a Message Generator (MG) in the SAS 21, where a header is added. The EMMs are passed to a Message Emitter (ME) as complete EMMs. The Message Generator determines the broadcast start and stop time and the rate of emission of the EMMs, and passes these as appropriate directions along with the EMMs to the Message Emitter. The MG only generates a given EMM once; it is the ME which performs cyclic transmission of the EMMs.

On generation of an EMM, the MG assigns a unique identifier to the EMM. When the MG passes the EMM to the ME, it also passes the EMM ID. This enables identification of a particular EMM at both the MG and th ME.

In systems such as simulcrypt which are adapted to handle multiple conditional access systems e.g. associated with multiple operators, EMM streams associated with each conditional access system are generated separately and multiplexed together by the multiplexer 4 prior to transmission.

Encryption Levels of the Broadcast System

Referring now to Figure 3, a simplified outline of the encryption levels in a standard broadcast system will now be described. The stages of encryption associated with the broadcast of the digital data are shown at 41, the transmission channel (eg a satellite link as described above) at 42 and the stages of decryption at the receiver at 43.

The digital data N is scrambled by a control word CW before being transmitted to a multiplexer Mp for subsequent transmission. As will be seen from the lower part of Figure 3, the transmitted data includes an ECM comprising, inter alia, the control word CW as encrypted by an encrypter Ch1 controlled by an exploitation key Kex. At the receiver/decoder, the signal passes by a demultiplexer DMp and descrambler D before being passed to a television 13 for viewing. A decryption unit DCh1 also possessing the key Kex decrypts the ECM in the demultiplexed signal to obtain the control word CW subsequently used to descramble the signal.

For security reasons, the control word CW embedded in the encrypted ECM changes on average every 10 seconds or so. In contrast, the first encryption key Kex used by the receiver to decode the ECM is changed every month or so by means of an operator EMM. The encryption key Kex is encrypted by a second unit ChP using a personalised group key K1(GN). If the subscriber is one of those chosen to receive an updated key Kex, a decryption unit DChP in the decoder security module will decrypt the message using its group key K1(GN) to obtain that month's key Kex.

The decryption units DChp and DCh1 and the associated keys are held on a security module associated with the decoder, in this case the smart card 30 provided to the subscriber and inserted in a smart card reader in the decoder. The keys may b generated, for example, according to any generally used symmetric key algorithm or in accordance with a customised symmetric key algorithm.

As will be described, different keys may be associated with different operators or broadcasters as well as with the conditional access system supplier. In the above description, a group key K1(GN) is held by the smart card associated with the decoder and used to decrypt EMM messages. In practice, different operators will have different subscriber unique keys K1 (Op1, GN), K1 (Op2, GN) etc. Each group key is generated by an operator and diversified by a value associated with the group to which the subscriber belongs.

Different memory zones in the smart card hold the keys for different operators. Each operator may also have a unique key associated solely with the smart card in question and an audience key for all subscribers to the services provided by that operator (see above).

In addition, a set of keys may also be held by the manager of the conditional access system. In particular, a given smart card may include a user specific key K0 (NS) and an audience key K1 (C), common to all smart cards. Whilst the operator keys are generally used to decode EMM messages associated with broadcast rights, the conditional access manager keys may be used to decrypt EMM messages associated with changes to conditional access system in general, as will be described below.

The above description of the system shown in Figure 3 relates to the implementation of access control in a broadcast system in which transmissions are descrambled by a single decoder and displayed on a single television display. Referring to Figure 4, a first and second decoder configuration will now be described.

Decoder Configuration

As before, a decoder 12 receives scrambled broadcast transmissions via a receiver 11. The decoder includes a portable security module 30, which may conveniently take the form of a smart card, but which may comprise any ther suitable memory or microprocessor portabl device. The decoder 12 is connect d to a modem channel 16, for example, for communicating with servers handling conditional

access information and is also adapted to pass descrambled audiovisual display information, e.g. via a Peritel link 53, to a television 13.

The system additionally includes a dependent or slave decoder 50 adapted to communicate with the decoder 12, for example, via an IEEE 1394 bus 51. The decoder 50 may include a connection (not shown) to the receiver 11 or to another satellite receiver to directly receive scrambled broadcast transmissions. Alternatively, this information may be passed from the first decoder 12 via the connection 51.

The second decoder 50 is further adapted to function with a portable security module 52. The portable security module 52 may conveniently be implemented as smart card. However, any portable memory and/or microprocessor device as is conventionally known, such as a PCMCIA card, a microprocessor key etc. may be used. The operation of this module 52 in descrambling transmissions will be explained below.

The decoder 50 also includes a link 54 to a television display 55 used to display descrambled transmissions. Whilst the elements of the decoders 12, 50 and the displays 13, 55 have been indicated separately, it is envisaged that some or all of these elements may be merged, for example, to provide a combined decoder/television set.

Secure Communication between Decoders

As set out in the introduction, in order to avoid problems relating to management of subscription data, it is desirable that only a single subscription is opened for the owner of the two decoders 12, 50. In the case where the decoder 12 is the principal or first decoder in the system, smart card 30 will be personalised to receive the monthly exploitation key Kex as described above in relation to Figure 3. In order to enable the decoder 50 to descramble and display a transmission via the display 55 it will be necessary to communicate certain information from the security module 30 to the security module 52 to enable this descrambling to be carried out.

In the present embodiment, the smart card 30 decrypts the ECM messages associated with a transmission so as to obtain the control word CW value. This control word value is then communicated in an encrypted form via the link 51 to the decoder 50 and smart card 52, where it is used by the decoder 50 and smart card 52 to descramble the transmission and display the programme via the display 55.

Embodiments other than this control word embodiment may nevertheless be envisaged, for example, in which a copy of the monthly exploitation Kex is passed to the decoder and smart card 50, 52 to enable the decoder 50 to operate independently thereafter.

As will be appreciated, in order to avoid any problems of fraud, it is essential that control word information or, indeed, any other information used in decrypting and descrambling a transmission, is never transmitted in a clear form over the link 51.

There will now be described with reference to Figures 5 and 6, a method for enabling such a secure communication link to be implemented.

For the sake of clarity, all encryption operations using a public/private key algorithm are indicated by means of the symbol f_a, whilst all operations using a symmetric algorithm are indicated by the symbol f_s. Decryption operations are indicated as f_a^{-1} or f_s^{-1}.

Private/public keys pairs may be generated in accordance with any suitable asymmetric encryption algorithm such as RSA or Diffie-Hellman. Symmetric keys may be used with algorithms such as DES. In some cases, custom symmetric algorithms may also be used.

Referring to Figure 5, the smart card 52 for the decoder 50 is personalised with a public key KpubMan shown at 65 and equivalent to the public key associated with a private management key KpriMan shown at 61. In practice, all smartcards 52 intended for use with dependent or slave decoders will include the k y KpubMan.

This personalisation step will be normally carried out in private at the headquarters of the system manager, either at the mom nt of first personalisation of the card (if it is already envisaged to provide a second decoder) or when a user demands the inclusion of a second decoder in his subscription.

Subsequently, the system manager possessing the secret private key KpriMan shown at 61 will communicate in a dedicated EMM message 62 a certificate Ct(KpubT) shown at 63. The certificate is prepared by encrypting a public key KpubT with the private manager key KpriMan. The EMM further includes a private key KpriT shown at 64 and stored together with the certificate Ct(KpubT) in the non-volatile memory of the smart card 30.

This EMM is itself encrypted in the normal manner for EMMs dedicated to one decoder using appropriate transmission or exploitation keys, such that only the decoder 12 and card 30 may decrypt this EMM message.

At the moment when the two decoders are put in communication via the IEEE 1394 link 51, the smart card 30 sends the certificate Ct(KpubT) to the smart card 52 as shown at 66. Using the public key KpubMan, the card decrypts the certificate at 67 to obtain the public key KpubT as shown at 68. This public key KpubT will thereafter be uniquely associated with the pairs of decoders 12, 50 and cards 30, 52.

The card 52 thereafter generates a random key value Ks shown at 69. As will be described, this random key is later used as a session key in conjunction with a symmetric algorithm to encrypt messages communicated in both directions between the cards 30, 52. A new session key value may be generated at every subsequent re-connection of the decoder 50 and card 52 in the system, i.e. every time the decoder 50 is switched on by a user, or at every viewing session, for example, of a pay per view film.

The symmetric key Ks is encrypted at 70 using the public key KpubT and the encrypted value sent at 71 to the smart card 30. The card 30 decrypts the message at 73 with the private key KpriT and stores the session key value at 72. As will be understood, in view of the nature of private/public

encryption algorithms the encrypted message may only be decrypted by a card possessing the private key KpriT, that is, by the card 30.

As described above, the cards 30, 52 are programmed by the same system manager who embeds or communicates the values KpriT, Ct(KpubT) and KpubMan to the respective cards 30, 52. In a further realisation (not shown) a second layer of authorisation may be provided using a system private key KpriSystem. In this realisation, a certificate Ct(KpubMan) comprising the key KpubMan encrypted by KpriSystem is stored in the card 30.

In such a realisation, the card 52 further possesses a secondary system public key KpubSystem. In operation, the card 30 sends the encrypted value of certificate Ct(KpubMan) to the card 52 which decrypts this message using KpubSystem to obtain KpubMan. Thereafter, the steps are the same as above, with the card 52 using the key KpubMan to obtain KpubT etc.

Turning now to Figure 6, the steps involved in the secure communication of control word information from the card 30 to the card 52 will now be described.

In normal operation, the slave decoder 50 and card 52 receive a scrambled transmission together with the encrypted ECM messages containing the control word information necessary to descramble the transmission. These ECM messages are passed at 75 via the IEEE 1394 link to the master decoder and card 12, 30. Alternatively, the ECM messages for a transmission that will be displayed via the slave decoder may be received directly by the master decoder and card 12, 30.

The card 30 then carries out at 76 a standard verification step to check that one or both of the decoders have the rights to access this transmission. In the event that the decoders do not have the necessary rights the "non-valid" message 77 is returned to the decoder and card 50, 52 and the process stops.

Assuming the subscriber possesses the necessary rights, the ECM message shown at 79 and containing the encrypted control word CW is then decrypted at 80 using the monthly exploitation key Kex shown at 81 associated with the system manager or operator.

The clear value of the control word shown at 81 is then re-encrypted at 82 using the previously obtained session key Ks shown at 83. As will be understood, the encryption algorithm used at 82 for the re-encryption of the control word need not correspond to that used at 80 and, indeed, for security reasons a different algorithm may be used. Conveniently, a custom algorithm proprietary to the system manager may be used for steps relating to the exploitation key Kex including the decryption step shown at 80 and a generic algorithm such as DES used for the encryption of session messages shown at 80.

In some cases, additional information, such as copyright notification information may be introduced between the steps 81 and 82, such that the control word CW and this additional information are encrypted by Ks and sent to the second decoder and card. The presence of such information is more important in cases where the second decoder is capable of recording the data or of passing the information to a recorder. The copyright notification may be used as a flag to prevent the second decoder from recording the data or from recording and playing back the data an infinite number of times, for example.

The encrypted control word is returned to the decoder 50 and card 52 as shown at 83. Using the equivalent session key Ks shown at 84, the card decrypts the message at 85 to obtain the control word in clear shown at 86. Thereafter, this control word value is used by the decoder and card 50, 52 to descramble the associated section of a transmission for subsequent display on the associated television display 55.

In some cases, it may be envisaged that the decoder 50 and card 52 may wish to pass information to another audiovisual device, such as a VCR. In such an example, the decoder 50 and card 52 may be supplied with the necessary private keys to assume the role of a "master" device and the same

operations carried out, mutatis mutandis, between the decoder and the other device to set up a secure link.

Whilst the use of a changing session key increases the level of security, other realisations can be envisaged where a constant session key is used or where the public/private keys KpubSIM/KpriSIM are used to directly encrypt information communicated from the decoder 50 to the decoder 12. The session key may itself comprise a private/public key pair.

Furthermore, whilst the data communicated from the decoder to the recorder comprises the control word in the described example other information may be passed via this link, even including information not related directly to descrambling a transmission.

Equally, the same principles as set out above may be applied to communications between other digital audiovisual devices connected in a network, such as digital VCRs, digital televisions or any combination of such devices.

Finally, whilst the above description has focused on the validation and communication of information in relation to a pair of decoders, the invention may equally expanded to cover a series of interconnected decoders, for example, a single master decoder possessing a plurality of private transport keys KpriT for decryption of messages from a plurality of dependent decoders each possessing its equivalent public key KpubT.

CLAIMS

1. A method of providing a method of providing secure communication of information between at least a first and second digital audiovisual device (30, 12 ; 50, 52) and characterised in that the second device (50, 52) receives a certificate (Ct) comprising a transport public key (KpubT) encrypted by a management private key (KpriMan), the second device (50, 52) decrypting the certificate using an equivalent management public key (KpubMan) and thereafter using the transport public key (KpubT) to encrypt information sent to the first device, the first device using an equivalent private key (KpriT) to decrypt the information.

2. A method as claimed in claim 1 in which the transport private/public key pair (KpriT, KpubT) are uniquely associated with the first and second device (30,12 ; 50, 52).

3. A method as claimed in any preceding claim in which the encrypted information sent by the second device (50, 52) comprises a session key (Ks).

4. A method as claimed in claim 3 in which the session key (Ks) is a key generated by the second device (50, 52) and usable in conjunction with a symmetric encryption algorithm.

5. A method as claimed in claim 3 or 4 in which the session key (Ks) is used by the first device (12, 30) to encrypt control word information subsequently communicated to the second device (50, 52).

6. A method as claimed in claim 8 in which the second device (50, 52) decrypts the control word information using the equivalent session key (Ks) and thereafter descrambles the section of a scrambled transmission associated with this control word.

7. A method as claimed in any preceding claim in which the first and second devices (50, 52 ; 12, 30) comprise a respective first and second portable security module (52; 30).

8. A method as claimed in any preceding claim in which the second device (50, 52) receives a system certificate comprising the management public key (KpubMan) encrypted by a system private key (KpriSystem), the second device (50, 52) decrypting the system certificate using a system public key (KpubSystem) so as to obtain the management public key (KpubMan) used thereafter to decrypt the encrypted transport public key (KpubT).

9. A method as claimed in any preceding claim in which the communication link between the first and second devices is implemented by a bus connection.

10. A method as claimed in any preceding claim in which the first and second digital audiovisual devices comprise a first and second decoder.

11. A method as claimed in claim 10 in which the first and second decoders (12, 30) are adapted to receive digital television transmissions.

ABSTRACT

METHOD AND APPARATUS FOR SECURE COMMUNICATION OF INFORMATION BETWEEN A PLURALITY OF DIGITAL AUDIOVISUAL DEVICES

The present invention relates to a method of providing secure communication of information between at least a first and second digital audiovisual device 30, 52 and characterised in that the first device 30 communicates to the second device 52 a certificate Ct(KpubT) comprising a transport public key KpubT encrypted by a management private key KpriMan, the second device 52 decrypting the certificate using an equivalent management public key KpubMan and thereafter using the transport public key KpubT to encrypt information sent to the first device, the first device using an equivalent private key KpriT to decrypt the information.

The present invention is particularly applicable to a method of providing secure communication between a first and second decoder.

[Figure 5]

1/6

Fig.1.

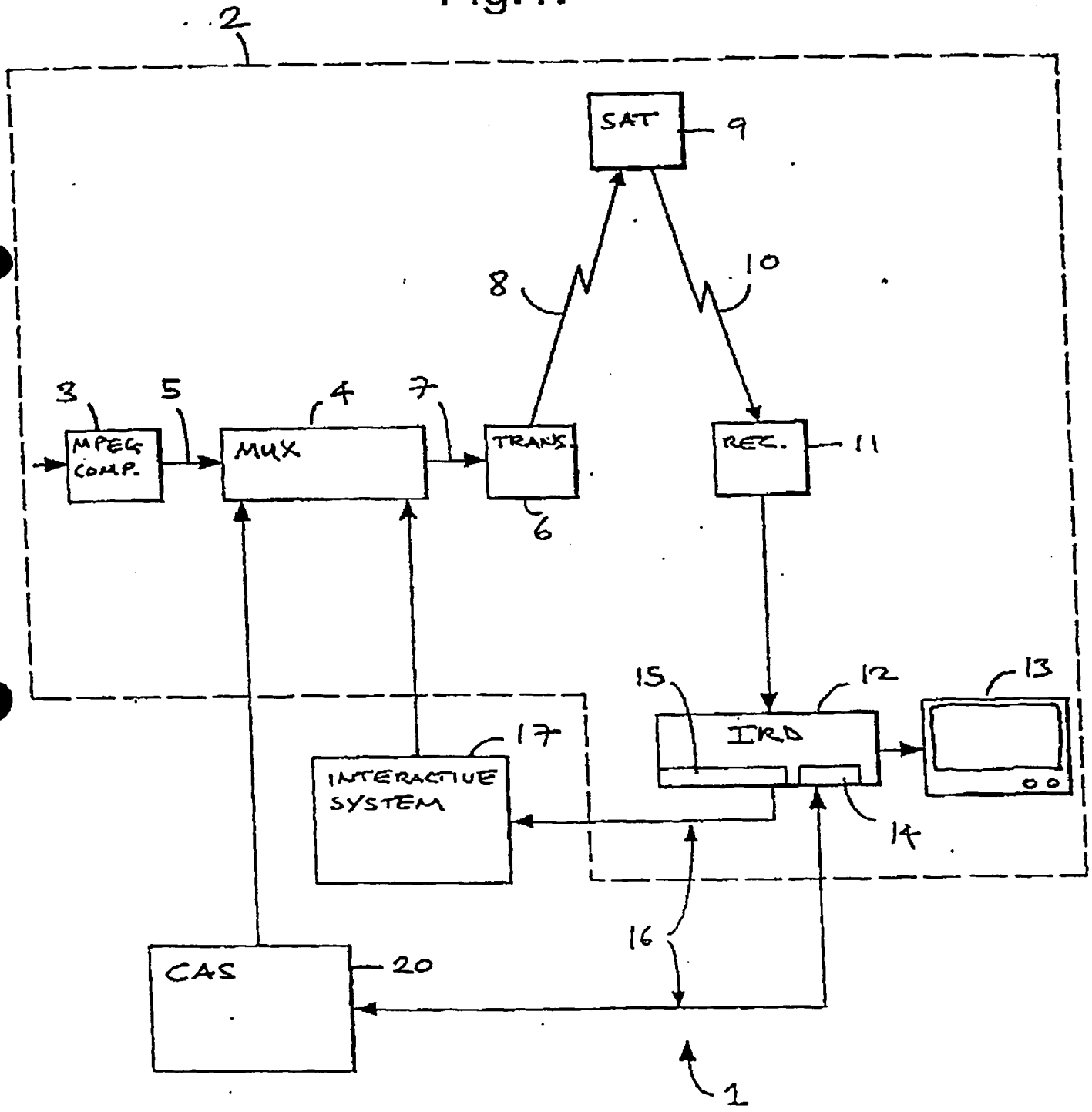
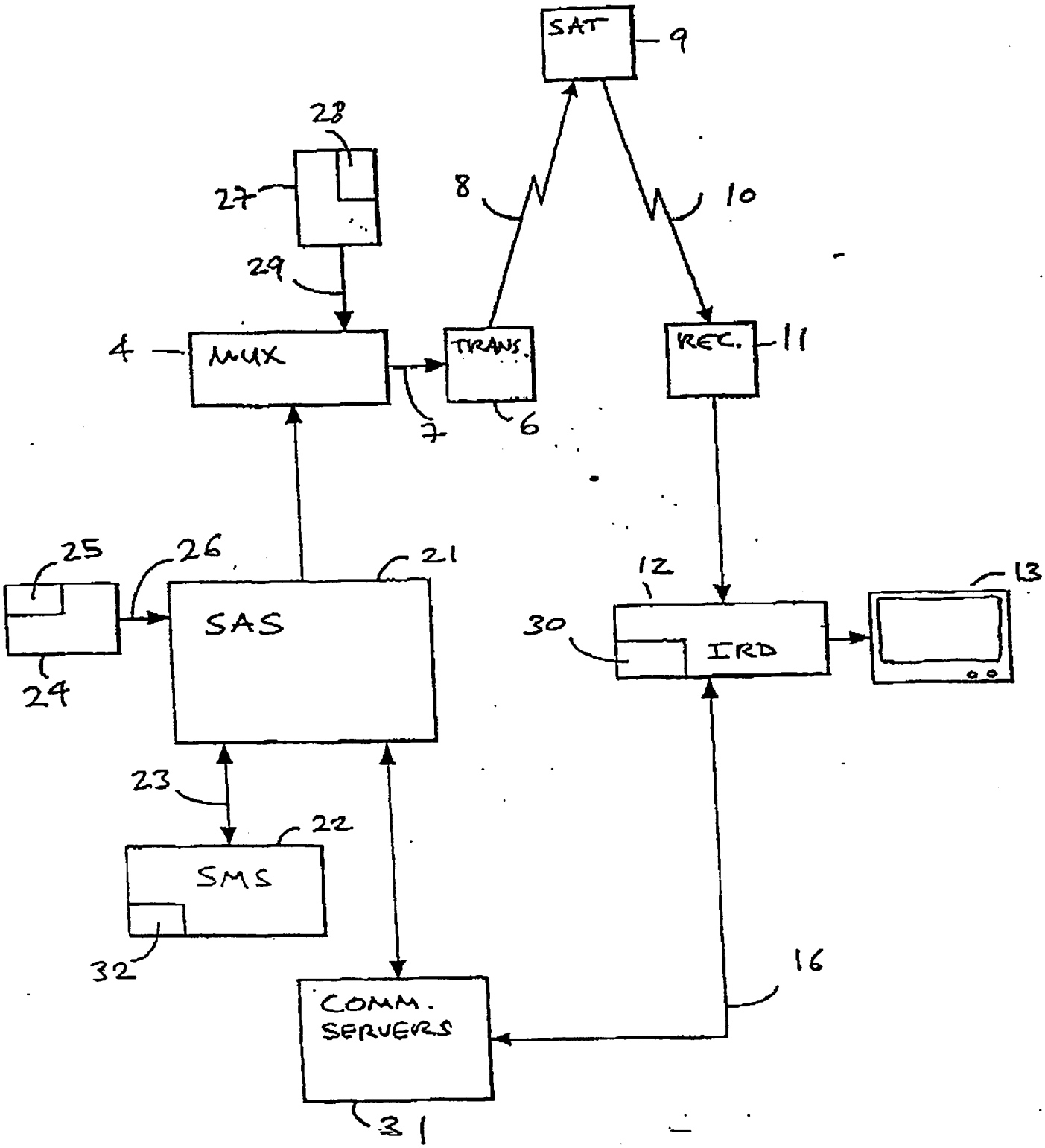
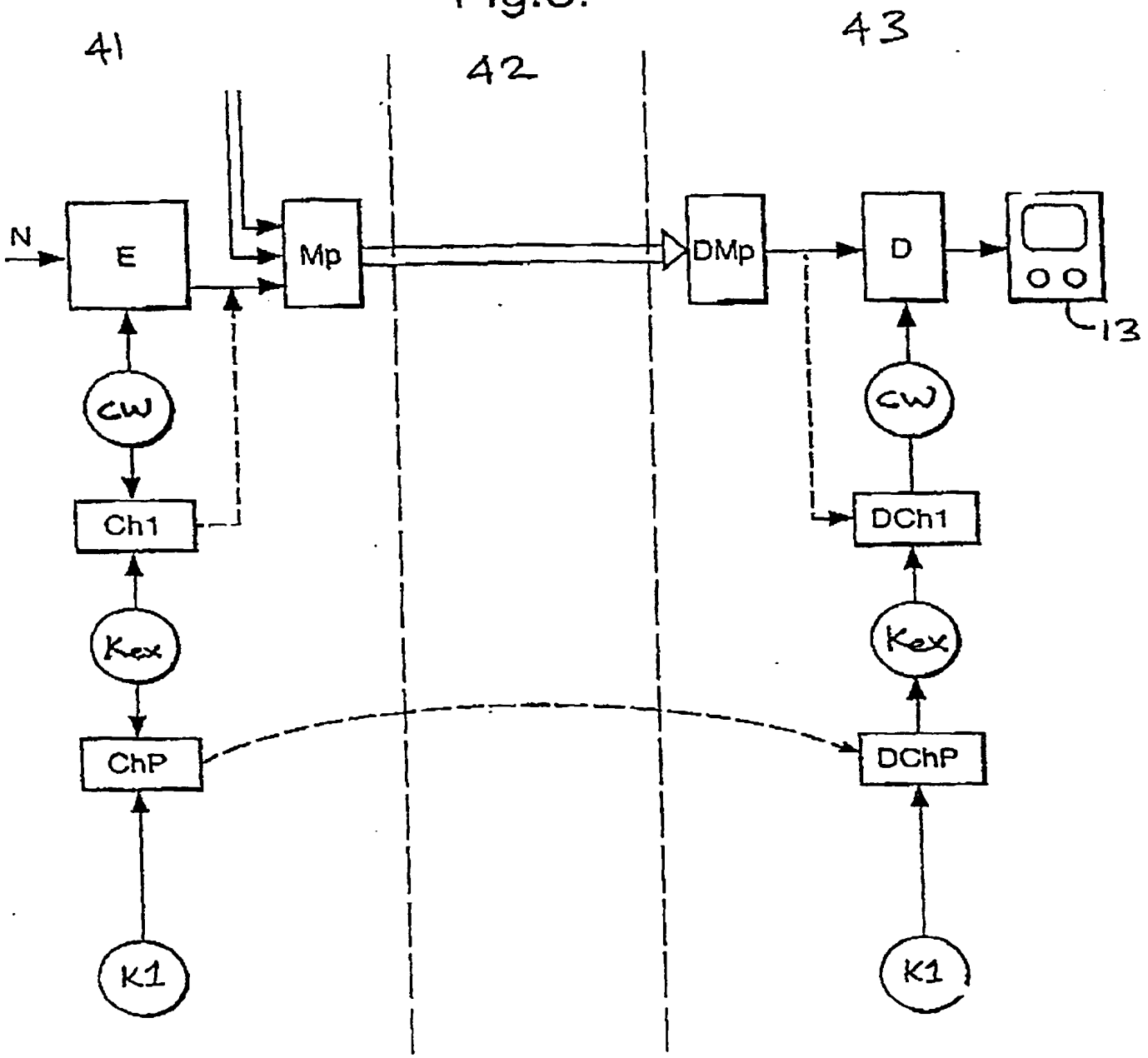

2
SAT
9
8
10
3
5
4
7
MPEG COMP.
MUX
TRANS.
REC.
11
6
15
12
13
IRD
17
INTERACTIVE SYSTEM
14
16
CAS
20
1

Fig.2.


SAT
9
28
27
8
10
29
4
MUX
TRANS.
REC.
11
7
6
25
26
21
12
13
SAS
30
IRD
24
23
22
SMS
32
16
COMM.
SERVERS
31

3/6

Fig.3.


41
42
43
N
E
Mp
DMp
D
13
CW
CW
Ch1
DCh1
Kex
Kex
ChP
DChP
K1
K1

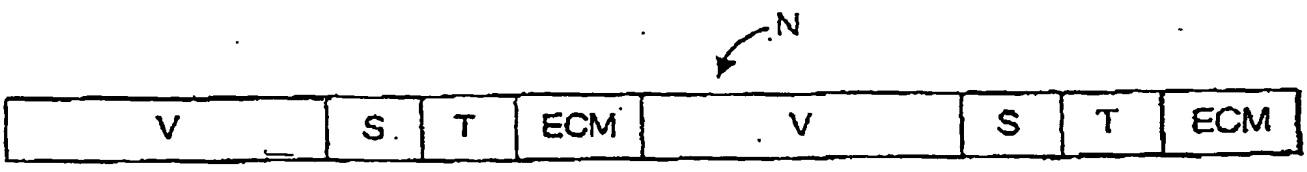
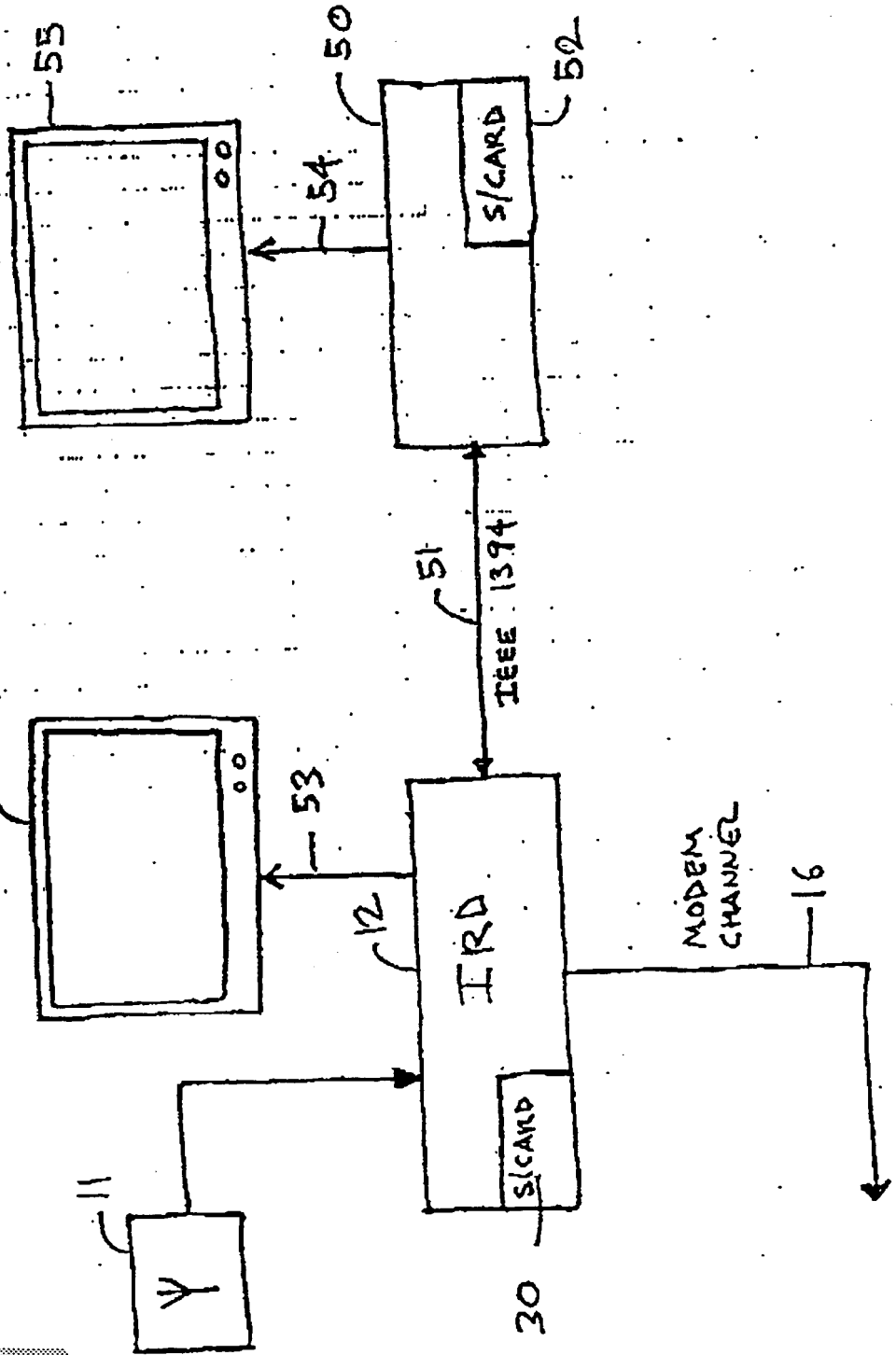

N
V
S
T
ECM
V
S
T
ECM

Figure 4


55
50
52
54
S/CARD
51
IEEE 1394
13
53
12
IRD
MODEM CHANNEL
16
S/CARD
11
30

5/6

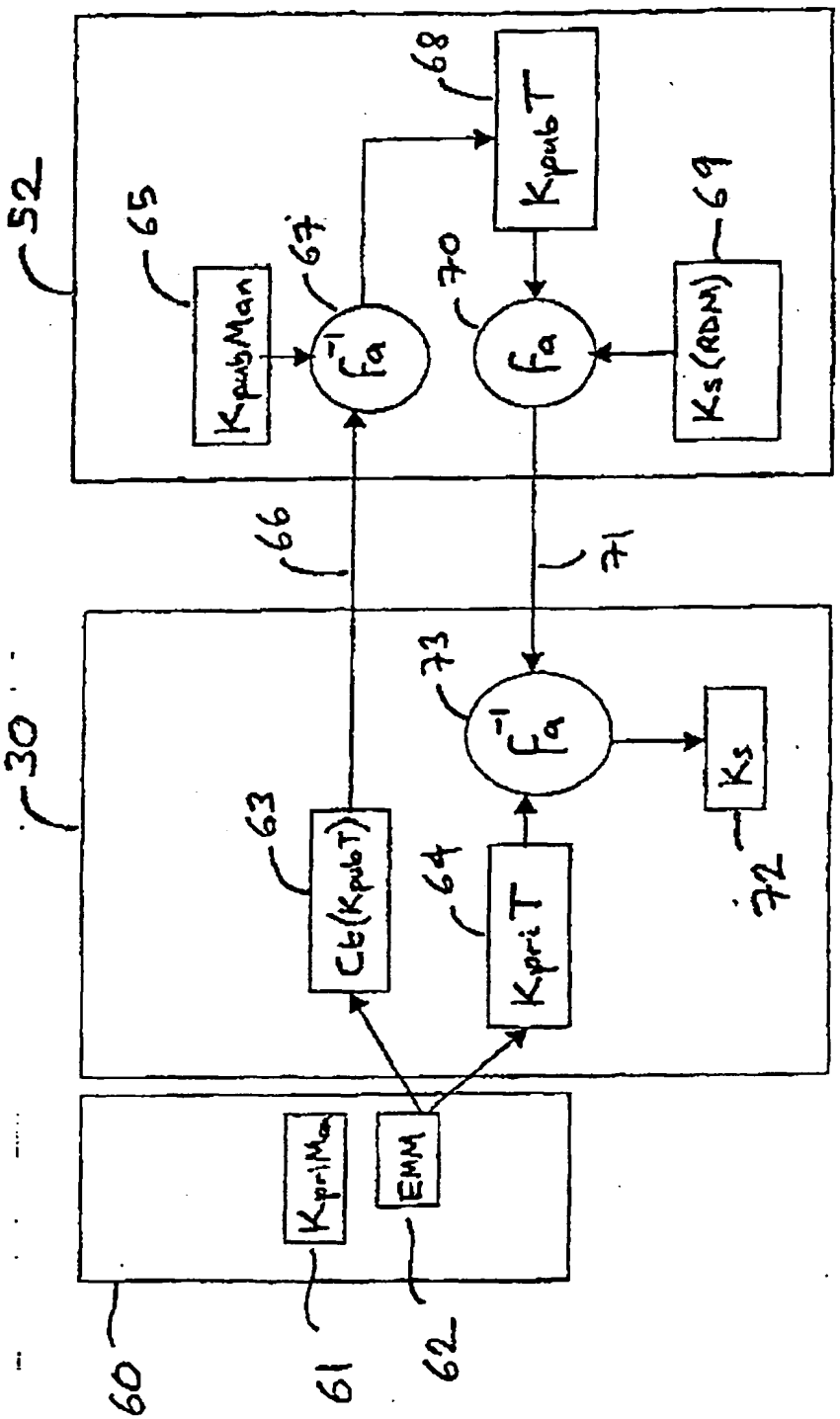
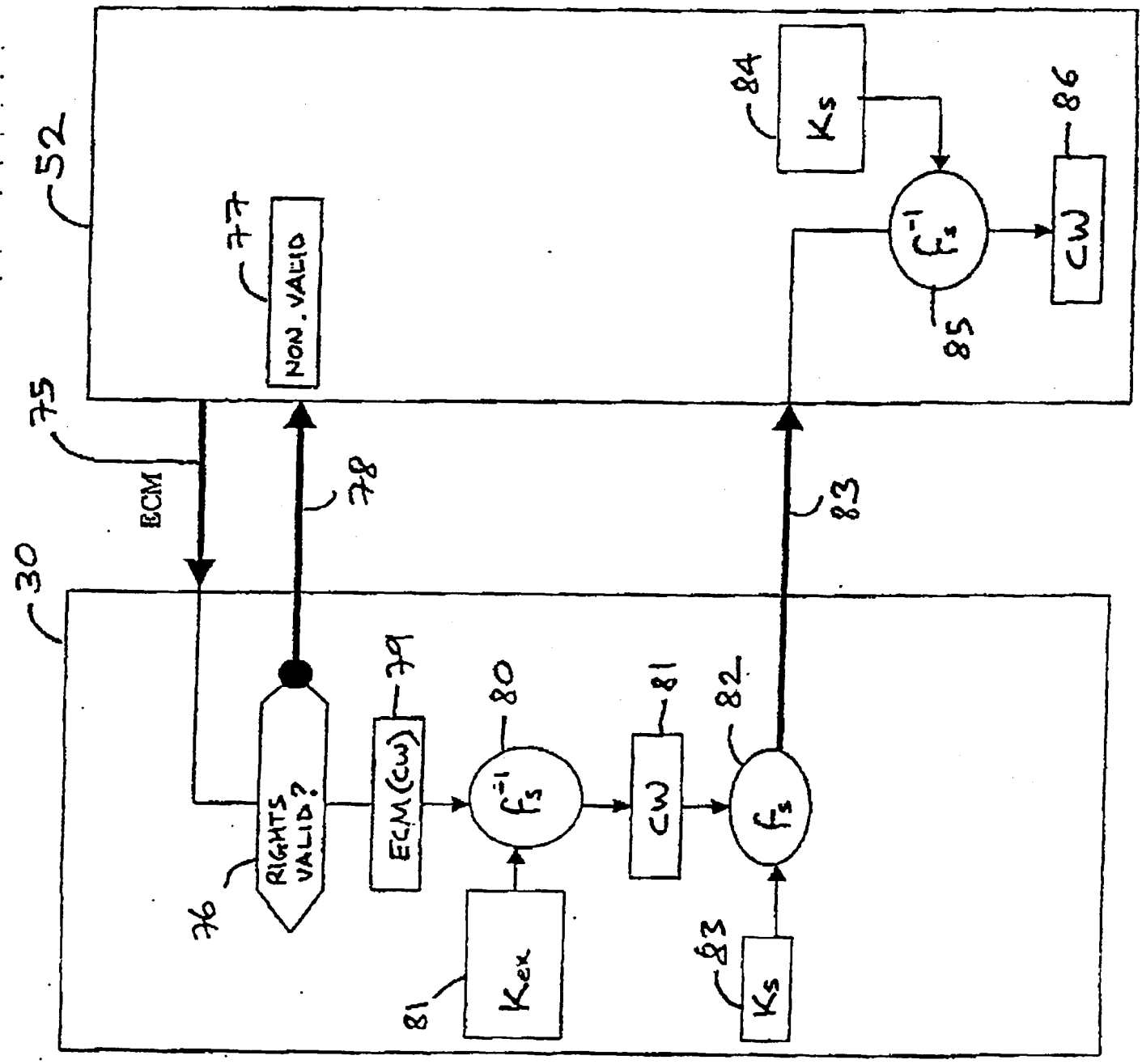

52
65
K_{pubMan}
67
f_a^{-1}
68
K_{pubT}
70
f_a
69
K_s (RDM)
66
71
30
73
f_a^{-1}
K_s
72
63
$C_E(K_{pubT})$
64
K_{priT}
K_{priMan}
EMM
60
61
62

Figure 5

Figure 6


52
77
NON. VALID
84
Ks
86
CW
85
75
ECM
78
83
30
RIGHTS VALID?
76
79
ECM(CW)
80
81
CW
82
Kex
81
83
Ks